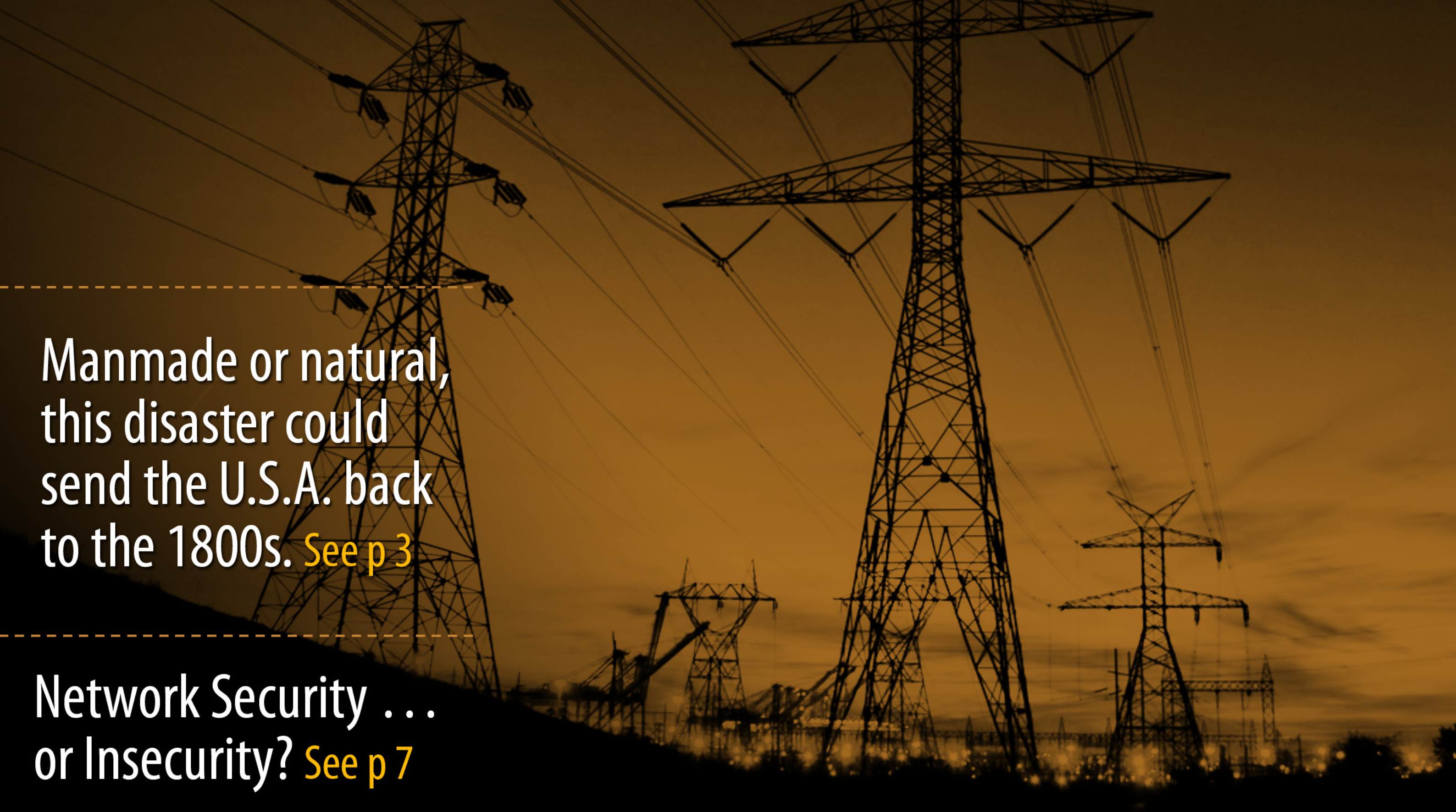
BLACK OUT

The Top 10 Threats To the Power Grid



Manmade or natural, this disaster could send the U.S.A. back to the 1800s. See p 3

Network Security . . . or Insecurity? See p 7

Is the power grid spying on you? See p 15

Published By:
Off The Grid News
www.OffTheGridNews.com
info@offthegridnews.com

Table of Contents

Threat #1: A Crippling EMP Attack

"Airplanes would literally fall from the sky, cars and trucks would stop working, and water, sewer, and electrical networks would fail."

It sounds like something from an apocalyptic Hollywood movie – but the threat is very real. That threat is EMP, short for electromagnetic pulse as well as HEMP, a newer term, which stands for high-altitude electromagnetic pulse. In a report recently released by the Heritage Foundation, a leading U.S. think tank, national security experts warned President Obama about the potential EMP threat from hostile nations or even terrorists.

A nuclear bomb detonated high above the earth's atmosphere wouldn't have its energy converted to blast energy by the atmosphere. So it can't destroy people or property directly. Instead, the bomb's energy would go out as electromagnetic energy, or an EMP. This could severely damage, if not completely destroy the electrical power grid. An EMP weapon would also destroy all things electronic – airplanes, vehicles, communications networks, computers, and more.

The report, entitled EMP Attacks – What the U.S. Must Do Now, pulls no punches. The consequences of an EMP attack would be catastrophic. According to the report, "Food would rot, medical services would collapse, and transportation would become almost non-existent."

The resulting chaos that would ensue if that were to happen is nearly unimaginable. Unlike a nuclear bomb detonated at ground level, an EMP device would not kill the surrounding population immediately. Instead, it would destroy the grid, returning America to a pre-industrial level of technology. Millions of people would suffer slow, agonizing deaths from starvation, lack of clean water, and lack of medical care.

While hostile nations may have the capability for a large-scale EMP attack, even a "smaller" EMP attack by terrorists would have catastrophic consequences. A nuclear bomb capable of producing an EMP can fit in a backpack and be launched from the back of a tractor trailer or from a shipping container on a cargo ship. An even smaller device called an explosively pumped flux compression generator (EPFCG)[1] could be carried by a single individual. In the hands of a terrorist, this device could release pulses in the millions of amperes and tens of terawatts, and it does it without a nuclear bomb.

An EPFCG set off in New York City could conceivably create an EMP that would stop the entire Northeast corridor cold. A single nuclear bomb, launched from a cargo ship in the Gulf of Mexico, could create a large enough EMP to destroy the electronics across over 90 percent of the United States.

Repairs to the grid would literally take years, if society could survive long enough to accomplish them. The equipment needed for these repairs isn't just sitting in warehouses, waiting to be used. In the meantime, with no power, cities and suburbs would become a very dangerous place to live. In a report put out by the DHS, an EMP attack of this type could ultimately cause the death of 90 percent of the U.S. population. People who live in the countryside, with access to arable land, well water, and who have alternative energy sources, would have the best chances for survival.

Threat #2: Devastating Solar Storms

While an EMP attack from a hostile power is possible, there's an equally devastating threat that's even more likely. And it doesn't come from any earthly power.

Approximately every 22 years, the sun enters a period of intense magnetic storms typified by the appearance of numerous sunspots. During these storms, the sun ejects plumes of hot gas and magnetic energy. One flare can contain the equivalent of one-sixth of the sun's total energy. And this happens in one second.

Most flares are small. But some are so powerful that they tear away chunks of solar mass. These chunks become balls of magnetized plasma, hurtling into space. These are called coronal mass ejections (CMEs). When they hit the Earth's atmosphere, they not only interact with our planet's magnetic field and cause the northern lights (aurora borealis), but they also threaten satellites and astronauts with intense radiation bursts. In 1958, a massive CME produced northern lights that could be seen in Mexico.

CMEs don't just make pretty lights in the midnight sky. Huge CMEs can knock out power. On Friday March 10, 1989, astronomers witnessed a billion ton cloud of solar plasma (electrically charged gas) wrench itself from the sun's corona and head straight toward the Earth at a million miles an hour. On Sunday, March 12, the plasma cloud reached Earth's magnetic field, causing a geomagnetic storm. The northern lights in stunning shades of red, purple, and green could be seen as far south as Florida and Cuba.

This wasn't just a pretty light show. The magnetic disturbance created a geomagnetic-induced current, or GIC, in the ground beneath North America. When an EMP occurs on the high-voltage grid, large amounts of additional current – GIC – are induced in power lines. The current passes on to generators and transformers down the line. Since there is so much current in the system, transformers can overload, overheat, and fail —or sometimes even explode.

Just past 2:44 AM on March 13, 1989, Quebec's power grid crashed, cutting off nearly 2,000 megawatts of power to the northeastern U.S.[2] Six million people lost power for nine hours. Weather temperatures in some parts of Quebec were at a dangerous -15°F.

Though the 1989 storm was serious, Canada got off lightly. Geomagnetic field severity is measured in nanotesla per minute (nT/min). The 1989 storm only reached an intensity of about 480 nT/min. Solar CME storms have produced fields as large as 2000 nT/min. However, a solar storm on May 14–15 in 1921 that disrupted telegraphs across the country may have reached 4800 to 5000 nT/min.

It's Not a Question of "If" … It's a Question of "When"

Under direction of the Federal Emergency Management Agency (FEMA), the Metatech Corporation carried out a study of the North American grid's vulnerabilities to geomagnetic storms. According to the study's principle investigator, John Kappenman, the big reason the grid is vulnerable stems from the need to transmit large amounts of power over long distances cheaply. The fact that the grid is overstretched and overloaded makes the catastrophic multi-regional impact of a magnetic storm all the more likely.[3]

Current operating procedures used on the grid were adapted in the wake of the March 1989 event and are designed to boost operational reserves — but they still leave us with a gaping vulnerability. They do not prevent or reduce GIC flowing onto the grid.

One of the chief hardware vulnerabilities is the huge multi-ton extra-high voltage (EHV) transformers that dot switching yards throughout the country. Kappenman says that these giant pieces of vital hardware undergo welldocumented failure when surges cause them to overheat, melt, and burn (many are immersed in oil for coolant). Since it is impossible to repair them in the field, they must be replaced with a new unit.

Manufacturing lead times for these transformers are, at a bare minimum, one year, but three years is more the norm. The units are not made in the United States; they're made in China. With over 300 EHV transformers deployed throughout the country and at risk during a geomagnetic event, the threat of a geomagnetic storm as big as the Carrington Event in 1859, or the solar storm in 1921, borders on the apocalyptic.

Damage could be avoided, if ...

Much of the damage from a solar storm could be avoided if inexpensive, supplemental, neutral ground resistors were installed to harden transformers against GIC.[4]

Kappenman argued in a statement to the Department of Homeland Security that:

> "A hardening program that expends even as much as $1 billion to protect the U.S. power grid against a severe geomagnetic storm, an event that has occurred before and is certain to occur again, is still far cheaper than the costs of a widespread blackout to the U.S. economy."

At this writing, it's been more than 25 years since solar storms crashed the Quebec grid in 1989. Since then, there have been a series of intense solar magnetic storms between 2011 and 2013.[5] We were fortunate in that case that the EMP from the storms missed the Earth. Had they hit the Earth, the National Academies of Sciences says it would have taken four to ten years – at a cost of $1 to $2 trillion – to restore the grid.

> "Within 12 months of an EMP attack or a massive solar flare, between two-thirds to 90 percent of the U.S. population would perish."

Congress created an EMP commission to look into the threat. The findings were grim. According to a report issued by the commission, "Within 12 months of an EMP attack or a massive solar flare, between two-thirds to 90 percent of the U.S. population would perish."

In August 2010, during an unusual show of bipartisan support, the House of Representatives passed the GRID Act by unanimous vote. This crucial piece of legislation authorized the federal government to take emergency measures to protect some 300 giant power transformers around the country. The bill died in the Senate.

At this writing, no further GIC hardening program for the grid has been announced.

Threat #3:
Cyber Security – Malicious Code

Imagine that you're relaxing at home after a long and chaotic day when suddenly, for no apparent reason, your lights go out. Not only do you see that all the lights in the homes on your street are out, but you also discover the electricity is out for as far as you can see. About an hour later, power comes back on and you learn from local TV news that, while power was out in a 300-mile radius for a period of time, other areas did not lose power.

Twenty minutes later, your power goes out again. An hour later, it comes on. Again, TV news reports the same thing: While most had their power out, a few areas reported their power had remained on. Twenty minutes later, your power is out again. And the entire cycle repeats for 6 more hours throughout the night.

Something weird has happened.

As you go about your daily business,

reports come in from around the country. Most regions have fluctuating power. Phone and cell service is sporadic; radio, cable, satellite and broadcast TV are also touch and go. Your drive to work is frustrating, long, and dangerous because there are no traffic signals working. When you get to work, you find the majority of computers running on battery backup only. But it doesn't matter anyway. Though major Internet service providers are operating, many local nodes and service providers are offline. Stock trades are delayed by two hours. All on-line banking, ATMs, and credit card processors have suspended operations.

And it doesn't stop there. Some major power lines have reportedly melted in places, causing large forest fires. Much of the Northeast is without 911 service, while parts of the Midwest and California can't muster enough power to regulate traffic. Las Vegas and much of Los Angeles are without power. The Grand Coulee Dam and Hoover Dam have shut down to avoid overloading their power switching yards.

By mid-morning, Homeland Security reveals that a cyber-attack on the nation's electrical grid occurred during the night because of a software worm. As proof, it releases NASA night-time satellite photos. These photos show the typical night-time glows from 14 U.S. cities turning into a series of smiley-faces that flash on and off in 20 minute intervals.

Think that's too farfetched? Consider that the smart grid will expose two-thirds of the U.S. economy to unprecedented cyber-attack. Cyber-attacks don't just come through a virus in an email. They are cunningly calculated to take advantage of vulnerabilities in system components, telecommunication connections, and common operating systems found in modern energy systems.[6]

If you had any doubt that the threat of cyber-attack is real, these four incidents should convince you otherwise.

Exhibit A:

"Eligible Receiver 97" was a U.S. government exercise conducted from June 9-13, 1997. The National Security Agency's Red Team (playing the bad guys) sought to penetrate U.S. Pacific Command (U.S. PACOM) computers and servers to test their vulnerability. The Red Team only used widely available hacker tools (network-scanning software, intrusion tools, and password-breaking "log-in scripts") to enter PACOM's network. They also gained control access to electrical grids and 911 systems in nine U.S. cities.[7]

If they were able to do this with readily available, common hacker tools, what would a truly dedicated cyber-attack be able to do? What would a skilled hacker, who can go far beyond the capability of these common tools be able to do? The risk that this exercise demonstrated is greater than we can imagine.

Exhibit B:

In the spring of 2007, a sustained cyber-attack hit Estonian government computer systems over a period of weeks. While not the biggest European country, it was the most wired. Virtually all bank transactions were electronic, and 82 percent of all tax declarations were via Internet. Nearly every school used e-learning. Internet traffic to government websites normally totaled 1,000 visits per day. The denial of service attack barraged their system with 2,000 visits per second. Government web services ceased, and three of the biggest news organizations went offline. Financial operations shut down almost all ATMs and forced the largest bank, Hansabank, to close online banking operations. In response, Estonia closed large parts of its network to the outside world.[8]

Exhibit C:

In April of 2009, the Wall Street Journal published a story (later confirmed by the U.S. government) that cyber spies from China, Russia, and several other countries had gained access to the electrical grid. The spies also left behind programs that had the potential to disrupt the U.S. grid on command.[9] When informed of the pervasiveness of the breach, an anonymous former Homeland Security official was quoted as saying, "There are intrusions, and they are growing. There were a lot last year."

The North American Electric Reliability Corporation (NERC) warned that the electrical grid is not adequately protected from cyber-attack. Between late 2008 and April 2009, the Pentagon spent $100 million repairing cyber damage.

Exhibit D:

On April 8, 2010, state-owned China Telecom computers posted network routing instructions that diverted "massive volumes" of U.S. and other foreign Internet traffic through Chinese servers for 18 minutes. This included information traffic to and from U.S. government and military sites, including the Secretary of Defense's office, and some commercial websites. U.S. cyber-security experts warned the network diversion hinted at data mining and posed many – possibly malicious – activities.[10]

At first blush, it seems that only governments would have the capability to launch cyber-attacks. The truth is, of course, that anyone with a computer and the knowledge to use hacking tools and software (all readily available online) can learn how to infiltrate any security firewall. The shutting down of Estonia in 2007 turned out to be a unified effort (called "hacktivism") by ethnic Estonian Russians angry at the Estonian government for removing a bronze statue of a Russian soldier.

The attack was a distributed denial-of-service attack using zombie or "bot" personal computers that are located all over the world, including those hijacked without their owner's knowledge here in the U.S.[11]

It's almost impossible to overstate the potential security threats to the smart grid. Attacks can take the form of breaches, deliberate reconnaissance, vandalism, network hijacking, and implantation of malware. All require effective defenses.

Add to this the fact that these attacks are being equally committed by foreign governments, angry cyber-mobs, or bored teenagers. Installing a defense that can match the capabilities of such adversaries could become an endless cyber-arms race.

The DOE estimates that 60 percent of the U.S. Gross Domestic Product (GDP) is tied to the grid. That means that when the power goes off, two-thirds of the economy grinds to a halt, and each hour without electricity costs millions of dollars.[12] One way or another, those lost dollars come out of your pocket.

Threat #4: Stormy Weather – the Edge of Reliability

It hits the ground like a runaway freight train, eating up and spitting out everything in its path for two and a half miles. At 300 yards wide with 160 mph winds, nothing can stop it.

Each year, the U.S. experiences an average of 1,000 tornadoes, with the most powerful storms destroying whole towns and knotting up high-voltage transmission towers like twist-ties. While some power lines have backups in heavily populated areas, many rural parts of the country do not. When a tornado crosses paths with a 30-year-old high-tension line in parts of the Midwest or west Texas, whole regions can go dark for days.

Hurricanes are less destructive than tornadoes, but the destruction covers a much broader area. When large hurricanes, like Katrina and Sandy, hit regions of the United States, they can wipe out electrical service for the whole region.

Large amounts of power lines can be torn down, requiring months of work to rebuild. Even power poles and towers are subject to the possibility of destruction.

> "Intensive urban sprawl has stretched the grid out so tautly that a single weather event can have catastrophic consequences for entire regions of the country."

Most storm blackouts, however, come from far less spectacular weather. Usually, it's just a little summer thunderstorm or winter snowstorm. People think that lightning probably hit a tree or a power line a few blocks away and that the lights will be on in a few minutes.

But what's happening now with sky-high 21st century energy demand is that major disruptions to the power grid happen more frequently because the grid is stretched so thinly. In the last 30 years, intensive urban sprawl has stretched the grid out so tautly that a single weather event can have catastrophic consequences for entire regions of the country.

In December 2008, an ice storm in New England and upstate New York left over 100,000 people without power a week after it hit. In January 2009, another ice storm affecting Oklahoma, Arkansas, Missouri, Illinois, Indiana, and Kentucky caused power outages for 2 million people. Even ordinary summer thunderstorms can have a big impact. On August 5, 2010, a thunderstorm knocked out power to Maryland and northern Virginia, affecting 221,886 people for eight hours. It happened again a week later, affecting 101,003 people in the metropolitan Washington, D.C. area.[13]

So what happens when the really intense weather hits? Two weeks after Hurricane Ike hit Houston in 2008, almost one-fourth of metropolitan area residents were still without power.

And let's not forget Hurricane Katrina, the costliest hurricane ever recorded, which brought with it 30 confirmed tornados: 11 in Mississippi, 4 in Alabama, and 15 in Georgia. The storm initially left an estimated 2.3 million people without power and grew to 5 million from shortages in the natural gas industry (which spiked prices). Local power company repair crews were overwhelmed by the damage. A month later, with repairs mostly complete, Hurricane Rita came through the Gulf and once again cut power to a million consumers.

In 2013, the power grid received a "D+" grade on its report card from the American Society of Civil Engineers (ASCE). The power grid grade card rating means the energy infrastructure is in "poor to fair condition and mostly below standard, with many elements approaching the end of their service life." It further means a "large portion of the system exhibits significant deterioration" with a "strong risk of failure."

"America relies on an aging electrical grid and pipeline distribution systems, some of which originated in the 1880s," the ASCE report read. "Investment in power transmission has increased since 2005, but ongoing permitting issues, weather events, and limited maintenance have contributed to an increasing number of failures and power interruptions."

Severe weather is a fact of life. In the face of increasing demand with limited resources, consumers need to be prepared to be on their own for days at a time – perhaps even longer.

Threat #5:
The Not-So-Smart Smart Grid

Ever since the beginning of electric service in this country, energy has been available for one price all day long. The smart grid eliminates that. In reality, electricity rates fluctuate hourly during the day. Utilities want to pass real-time market pricing to the consumer so that they can warn consumers when prices are high and cut their energy use.

> "The smart meter, now being rolled out in markets across the country to millions of homes, is a key point of entry for malicious hackers."

One day in the not-too-distant future, it might look something like this:

You wake up on a fine, sunny, summer morning and get yourself ready to head out to work. You listen to the news as you sip your coffee and learn from the weather forecast that it will be extremely hot with highs in the upper 90s. Since your town is part of the smart grid with real-time pricing, you get on your computer to check your current usage and cost. With the price hanging at 10¢/

kWh, and knowing that your cost will go up during the day, you decide to set your thermostat to 80 degrees. Just before you leave, you unplug phone chargers, the home wireless system, dial up the refrigerator, turn off the de-humidifier, and reset the water heater to "vacation."

At work, you find your employer is equally aware of the day's electricity costs. Only some of the lights are on, and air conditioning is rationed, with priority going to servers and executives. Even the water cooler's chiller is turned off. At 11 AM, you visit the web address of your smart meter. You find that your electricity price has jumped to 12¢/kWh. You remotely set your air conditioner higher to 82 degrees. An hour later over lunch, you check again and your utility has broadcast a message offering a $2 rebate for access to your air conditioner's control cycle.

You decline, hoping the rebate will go up to $5 like last time.

And so the day goes, with more and more of your productive time being sucked away to chase and tweak the real-time price changes of your electricity.

Does it sound far-fetched? It's not. This could well be what life is like in the fast-approaching age of the "smart grid."

The Department of Energy has described the "smart grid" as a suite of technologies that will allow "customers and the utility to better manage electricity demand, and will include self-monitoring and automatic protection schemes to improve the reliability of the system." The smart grid will essentially function as both power grid and computer network.

This is where the Smart Grid's vulnerability lies. According to an article published on CNN.com, it would take a hacker with just $500 worth of equipment and knowledge of electronics and software engineering to take "command and control" of the smart grid's smart meter system. The smart meter, now installed in millions of homes across the country, is a key point of entry for malicious hackers.

Once in the system, a hacker could gain control of thousands, even millions, of meters and shut them off simultaneously. A hacker also might be able to dramatically increase or decrease the demand for power, disrupting the load balance on the local power grid and causing a blackout. These experts said such a localized power outage would cascade to other parts of the grid, expanding the blackout. No one knows how big it could get.[14]

Malware and viruses can also be introduced into the system to shut it down.

In theory, a smart grid allows power

Public Utility Commissions Field Smart Meter Complaints

- In Texas, one couple filed a lawsuit against Oncor, a transmission and distribution service provider. They claim that bug-riddled software that collects and manages the data from smart meters is inaccurately reporting their usage. The Public Utility Commission of Texas is investigating.[15]
- Customers of Central Maine Power, along with area doctors, are concerned that the frequency emitted by the smart meters is potentially harmful to health. Maine's Public Utilities Commission is reviewing a complaint filed by residents.[16]
- Almost two dozen local governments in California have demanded a moratorium on smart meter installation, citing health concerns. PG&E failed to do even a basic Environmental Impact Report, but the California Public Utilities Commission will not allow individuals to opt out of smart meter installation, even when severe health issues are involved.[17]

companies to have better control over power distribution, while consumers would have access to their own energy usage in real time. Utility companies insist that real-time pricing will save consumers up to 15 percent in energy costs. What they're not telling you is that the company's costs will be shifted onto their consumers' backs.

With real-time pricing, electric prices could spike from 10¢/kWh to 12.5¢/kWh – or more – depending on demand and fuel costs. That's a 25 percent increase for a period of 4 to 6 hours – every day. Since prices generally rise in the middle of the day when most people are at work, most consumers are not home to micromanage their home energy use.

Smart meters have replaced the humble meter reader in metropolitan and rural areas, often with an investment cost of several billion dollars. Guess who's paying that cost?

Most state public utility commissions allow utilities to pass on the expense of the smart meters as another fee on the monthly electric bill.[18] Pacific Gas and Electric of California installed 10.3 million smart meters, with an initial budget of $1.7 billion. However, problems with supplies, bugs in the networking technology, as well as performance failures by the meters, delayed the project and raised the costs. These additional costs have of course been passed on to consumers.[19]

Threat #6: Informers in your Home

The next threat on our list isn't a threat to the grid. It's how the grid threatens you – or, more specifically, your privacy. The smart grid will encourage the use of smart appliances. Smart appliances are self-monitoring and use their Internet connection to report their status to their owners. For instance, in a smart grid scenario in the very near future, your refrigerator could track its energy use and calculate its power consumption and operating cost for the day.

It can also take inventory of its contents through the miniature radio frequency (RF) transmitters on labels that are becoming increasingly common. Walmart pioneered the widespread use of RF transmitters in the retail industry a few years ago, and others have since jumped on the bandwagon. Stores use these labels to gather inventory information such as how many cans of peas are in stock, or the age of the boxes of mac-and-cheese. With a smart refrigerator, you don't need to open the door to see what you have and how old it is. It can read RF labels and show the entire contents of the refrigerator on a display on the door.

Your refrigerator could even put together a shopping list for you, featuring your favorite items on sale at your local grocery store. In a smart-grid scenario, your appliances "talk" about you and your family. Sure, it sounds convenient to have your refrigerator tell you when it's time to buy mustard, but a lot of information can be strung together from small pieces. Your refrigerator could report its entire contents to a data-collection company for use by different food marketing companies, including your local grocery store. It could report when and where an item was purchased, how often that item was used, and how long it lasted.

Big government snooping in your refrigerator?

With smart appliances, the amount of information collected on you and your family would be enormous. Smart TVs, Blu-ray players, and cable boxes could instantaneously report what you watch. Water heaters could report energy use and flow rates to show the number of showers a family takes.

Washers could report the amount of laundry through water amount, soil-selection type, and load size to identify certain lifestyle conditions and calculate how fast a household uses detergent. In the course of a year, a complete and intimate behavior profile could be assembled that would be used to predict your family's future behavior.

> "Air conditioners, heat pumps, refrigerators, freezers, and TVs could all be turned off remotely by the authorities without the owner's permission."

This behavior profile could be sold to anyone interested in having highly detailed consumer information.

It could also be used against you – by overzealous government officials who think they know what's best for you.

In December of 2010, Michelle Obama expressed concern about what children are eating today, and said, "We can't just leave it up to the parents." A refrigerator equipped with smart technology could report if you're buying and, by extrapolation, consuming your veggies. If a government can force you to buy health care insurance, they can also tell you what you have to eat. Smart technology gives them the ability to monitor compliance.

With a smart appliance, you risk control being taken away from you and put into the hands of a utility or the government. Remote bureaucrats in an air-conditioned office could decide how much electricity you get – if any. With the smart grid, when peak energy demand threatens regional grid stability, a utility or ISO (Independent System Operator) could theoretically reduce or kill power demand by directly ordering home appliances to shut down until a reactivate instruction is issued. That means air conditioners, heat pumps, refrigerators, freezers, and TVs could all be turned off remotely by the authorities without the owner's permission.

Imagine this. You've had a long day at the office where the air conditioning was turned off to conserve energy. You're hot, sticky, and irritable. When you unlock your front door and step inside, the house is hot and stuffy because your air home conditioning was also turned off.

Your smart refrigerator is urgently displaying warnings about cooling errors and spoiled food. No worries, though – because that same smart refrigerator is also telling you that the milk and ham you have to replace is on sale at the local grocery store.

While this sort of technology is being touted as a breakthrough in consumer convenience, we have to realize that anything which can be used for wrong will eventually be used for wrong. Government agencies or even corporations could create this sort of scenario, just for the purpose of stimulating sales, or even to cause people to buy something that has additional technology in it, allowing an even greater invasion of their privacy.

Ultimately, both the government and big business look upon the general public as only one thing ... a source of funds. Their goal is to see how much money they can milk from people, in order to fund their own activities. They really don't care if they are helping or harming the people they are getting the money from, as they don't feel any sense of responsibility towards them; after all, they are nothing more than someplace to take money from.

Threat #7: Big Business, Big Government, Big Mess

Who gets a say in how energy gets into your home? FERC, NERC, DOE, EPA, ISOs, RTOs, and a whole host of alphabet soup federal agencies, as well as utilities companies across the nation. Your home energy is smack-dab in the middle of a tug-of-war between competing entities.

Prior to the Energy Policy Act of 2005 (EPACT05), FERC (Federal Energy Regulatory Commission) had the power to approve transmission projects and establish rates. However, each proposed transmission right-of-way (referred to in the industry as "siting") had to be approved by each state that right-of-way entered. It was no big deal in western states. But projects in the Northeast often got bogged down and delayed in state approval procedures and red tape for years.

With EPACT05, Congress sought to streamline the whole mess. They put the grid under federal jurisdiction and gave FERC the ability to have final authority on state siting issues. It was a power grab for FERC – literally. The act enabled FERC to acquire rights-of-way by use of federal eminent domain powers to condemn private land.[20] But things still were not as simple as intended. If a state failed to act on a siting permit application within a year, or even rejected it, the transmission line developer could bypass the state process and bring its application to FERC for approval. Not so fast, said the Fourth Circuit Court of Appeals. It muddied the waters further when it ruled that a state's decision to reject a project could not be appealed to FERC because the commission does not have jurisdiction.

This has left several new transmission line projects in limbo. These projects are being fought by local residents. Even though FERC officials are paid by the taxpayer, they aren't working for them, as this situation clearly illustrates. FERC permits transmission companies in the midst of a project facing legal delays to recoup their legal expenses – by adding the tab to consumers' electric bills.

That's not the only clash between agency rules and government energy policies. Case in point: the North American Electric Reliability Corporation (NERC) is an international regulatory authority established by the FERC to evaluate reliability of the bulk power system in North America. Recently, it warned that impending EPA regulations endangered the production of 1,201 coal, gas, and oil steam-generating plants (responsible for generating about 252 gigawatts of power) and nearly one-third of all nuclear plants (about 60 gigawatts more).

In June of 2014, the EPA proposed new regulations on the emissions generated by coal-fired electric power plants. These new regulations (not laws passed by Congress) could also affect natural gas power plants. About 40 percent of the nation's electrical generating capability comes from coal power plants, with natural gas accounting for an additional 27 percent. So, these new regulations would have a major impact on the price of electricity, as well as the country's ability to produce electrical power.

The new regulations were supposedly written to attack the emissions of "greenhouse gases" by these power plants. However, for the sake of this regulation, the EPA has determined that carbon dioxide is a greenhouse gas. This is surprising, as all plant life breathes in carbon dioxide and breathes out oxygen, just as animal life (including humans) breathes in oxygen and breathes out carbon dioxide. It appears that there is no real reason for making this determination, other than to attack coal-fired power plants.

The coal-fired power plants are one of the older parts of the grid, with 63 percent of the plants being 40 years old or more; almost half of the existing coal-fired plants are over 50 years old, already having surpassed their expected life-expectancy. The new regulations supposedly are intended to make the older plants more efficient, so that they reach the emissions levels of newer plants. However, the actual emissions levels being required from these new regulations are based upon experimental technology which is not ready for installation in the power plants.

This will result in the power industry being required to shut down and replace most of these power plants, as retrofitting them with the new technology is not practical. In studies conducted by power companies, it would cost more to retrofit power plants, than it would cost to build new ones.

Ultimately, the true goal of these regulations isn't to make coal power cleaner, but to shut down the coal power industry, a stated goal of President Obama. This would mean less power to go around at a time when generation capacity is already stretched thin, increasing the likelihood of power shortages.

Regulations continue to be debated and contracts haggled over, while consumers are left, literally, to sweat it out until things are settled.

Threat #8: Fuel Prices – Up, Up and Away

It's economics 101. When demand for a commodity increases, the price goes up. This is a basic truth of the market whether that commodity is beef, soybeans, or fossil fuels such as natural gas and coal. Another truth is that many things can squeeze a commodity's supply and raise prices, including striking workers, new environmental regulations — or competing demand from a foreign country.

Old King Coal is Still King

The two biggest fuel sources America uses to generate electrical power are coal and natural gas.[21] Of the two, coal is the cheapest – but not for much longer.

America is the largest producer of "recoverable" coal, which means that the miners can get to the coal to mine it.

In 2009, nearly 1.075 billion tons was dug out of the U.S. coal fields.[22] Coal is divided into four broad categories: anthracite, bituminous, sub-bituminous, and lignite. Each group burns differently; some burn hot and clean, while others burn poorly. Coal that burns hot and efficiently goes to generate power in 47 states – including Hawaii.

The price of coal fluctuates. For example, on October 22, 2010, the commodity price of Powder River Basin coal was 0.7 cents/pound (yes, that's seven-tenths of one cent).[23] Because of its low cost and good quality, Powder River Basin coal is shipped to power plants as far away as California, Minnesota, and Texas.

"Dirt cheap" coal is a victim of its own success. Its low price drives higher demand … which drives up the price.

U.S. coal-fired power plants face another challenge, too. They now have serious competition for fuel. Coal exports are high and trending higher. Meanwhile, prices for higher-priced metallurgical coal for export (used in the production of steel) are also rising sharply. Why?

China, Japan (which imports every last nugget of its coal), South Korea, and India are burning through coal like crazy to generate power and satisfy the fuel-hungry demands of their growing economies. In September 2010, the largest coal producer in the U.S., Peabody Energy, announced it would ramp up its efforts to export more Powder River Basin coal to Asia by building a terminal on the Columbia River in Washington state.[24]

Even though China is the largest producer of coal in the world, they still can't get enough cheap coal to meet their needs. U.S. coal prices, meanwhile, are still a relative bargain for hungry China. How is this possible? Since coal trades on the international market in U.S. dollars, and the dollar is so devalued, China imports U.S. coal more cheaply than it would otherwise have to spend in order to mine its own coal. Both Japan and India are reaping the same benefit.

In the meantime, utility companies are between a rock and a hard place. They must make costly efficiency improvements to their power plants in order to satisfy new EPA regulations. That requires taking on enormous amounts of debt to afford these improvements. That in turn puts them in a precarious financial position. But if they don't take on the debt to make improvements, they won't stay competitive in the energy market ... in fact, they won't even be able to stay open. Meanwhile, they're risking financial ruin when commodity prices shoot up.

But there's always natural gas, right?

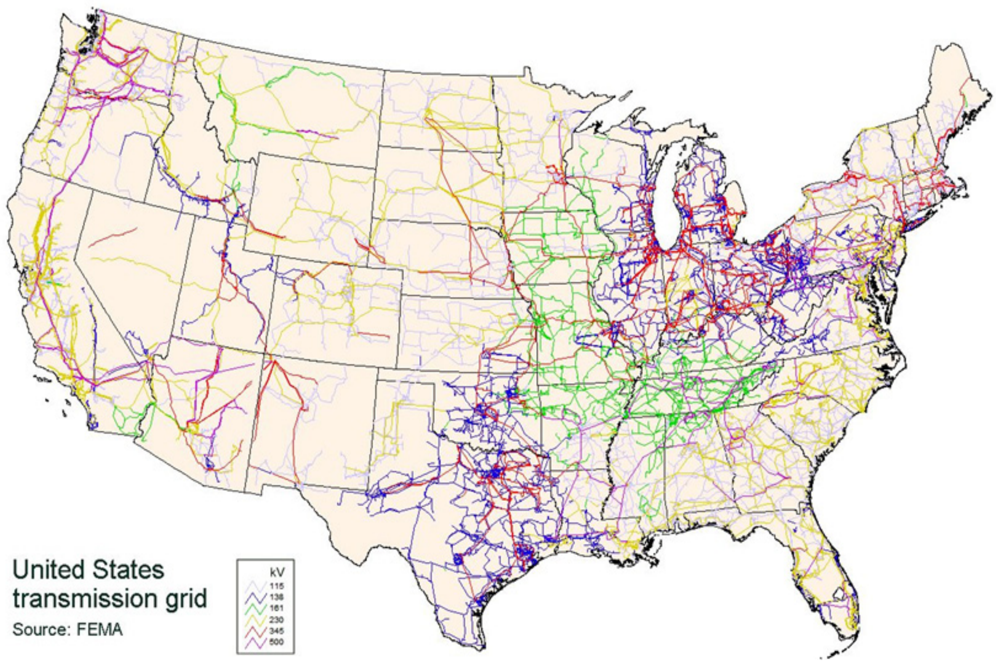
Natural Gas Snafu: All Fracked Up

Natural gas is more expensive than coal, but it burns cleaner. Nationally, it generates a little more than one-fourth of the U.S. supply for electricity, especially in Texas and the Gulf Coast where it's practically in their backyard. The price has remained low due to low demand and high amounts in storage. Because of the low price, many utilities are changing over their generator fuel to natural gas. They also believe that the price of natural gas will remain low and may dip well below coal's price. Unfortunately, that belief may just be so much … gas.

Natural gas was known for years to exist in the underground shale layers in much of North America. Buried beneath the states of Virginia, West Virginia, Ohio, Pennsylvania, Maryland, and New York lay one of the country's largest shale gas fields: the Marcellus Shale. It's been called a "Super Giant Gas Field" with possible reserves running as high as 500 trillion cubic feet (cu ft). Similar estimates showed the Barnett Shale in Texas to hold nearly 50 trillion cu ft. Industry experts claimed enough natural gas to supply the U.S. for two years, have a worth of $1 trillion, and make the U.S. a net exporter of natural gas. The trick lay in how to get at it.

One technical innovation breakthrough helped drive natural gas prices lower: horizontal drilling. Horizontal drilling technology utilizes a steerable drill that can turn and bore in any direction, powered below ground surface by hoses from hydraulic pumps. When the drill reaches a shale gas deposit, hydraulic fracturing chemicals and water are pumped at high pressure. The fluid fractures the shale (called "fracking") and pushes the natural gas into the well and up to the surface.

In July 2008, market speculation pushed gasoline to over $4 per gallon and natural gas prices to $13.69 per billion British Thermal Units (mmBTU). Electricity rates in some southern states exploded. Smelling huge profits, every company with a horizontal drilling rig rushed off to frack shale.



By September 2008, as the financial crisis killed investments and jobs, energy prices slid. By September 2009, natural gas prices dipped lower than a deflated hot air balloon. From $13.69/mmBtu prices sank by a whopping 80 percent, to only $2.409 per mmBTU. Suddenly, there was so much natural gas in storage that ships loaded with liquefied natural gas had no port to deliver it.

For the next several years, the price of natural gas remained relatively steady.

So how do low natural gas prices threaten the grid? For starters, estimated gas reserves might only be hype. One industry poster-child is the Kardell Gas Unit 1H, pumping in the Haynesville Shale in San Augustine County, Texas.[25] In October 2009, this well achieved a continuous 24-hour flow rate of 30.7 million cubic feet (Mcf) with a flow pressure of 6,824 psi. Impressive to be sure – but unique.

Most wells are like big balloons, yielding enormous amounts in their first year, but dwindling rapidly to only 25-50 percent of their initial amounts the following year. It is widely calculated that the actual average commercial life of a shale gas well is seven years. Some last no more than four.

> "The Energy Information Administration was forced to revise its shale gas production estimates. … Shale gas is looking more and more like an over-hyped gamble."

The Energy Information Administration (EIA) was forced to revise its shale gas production estimates, discovering the volume output was far less.[26]

Companies made massive investments in expensive equipment and mining rights in the hope that extracting fantastic amounts of natural gas would recoup their investment. They guessed wrong. All those hundreds of trillions of cubic feet of gas, unfortunately, just aren't there.

The bottom line: higher fuel costs – coal and natural gas – will get passed on to you, the consumer.

Threat #9: Transmission Capacity On Overload

Ever hear about the guy who started putting up a few Christmas lights on his roof and used a scrawny little extension cord? Every year, he put up more and more lights but kept using that scrawny little extension cord. One year, he put up so many lights that it looked like his house might be seen from space — until he plugged in that scrawny extension cord.

It melted and set fire to his house.

The official government report on the Great Northeastern Blackout of 2003 said that no utility had undertaken any major transmission project in over a decade. Now, more than a decade later, the same can still be said. Rather than improving the capability of the existing grid by adding more transmission capability, the electrical power industry is investing in better control of the existing transmission capability with the smart grid. Like the guy with his Christmas lights and his scrawny extension cord, utilities have been pushing the system harder and harder.

The 2003 report's conclusion reads: "The system is being operated closer to the edge of reliability than it was just a few years ago."[27] How much more true is that today, than it was when it was written?

Many sections of the grid in the U.S. are just like that scrawny extension cord. They are analogous to a single line transmitting huge amounts of power from city to city, and they're constantly monitored to prevent overload. Many are 80 years old. Power lines have a maximum safe load they can carry. Beyond it, they stretch, sag, break, or even melt. Overloaded power lines pose a threat to commerce and national security. The Department of Energy (DOE) estimates the annual cost of power outages to be $25 – $180 billion.[28] Transmission utilities are required to carefully manage instances when demand causes congestion. The power line wires themselves do not actually get congested. Rather, utility companies must wait to transmit power because so few lines are available. Picture three lanes of highway traffic trying to suddenly merge into a single remaining lane. Flow bogs down. According to the DOE, there are four congested areas in the U.S.: mid-state New York southward along the Atlantic coastal plain to northern Virginia; the urban areas of southern California; the San Francisco Peninsula; and the Seattle-Portland area.[29] While the FERC and its ISOs do their best to prevent abuse, it does happen, especially where state energy regulatory laws are overly complex.

Transmission companies can make a killing by deliberately overbooking the transmission schedules. Because of complex deregulation rules in California in 2000, the state paid congestion fees as an incentive for power providers to solve a congestion problem. During the California energy crisis, energy transmission companies profited from the rules by routinely scheduling more transmissions than they had capacity —even though the actual demand did not exist.

The answer to congestion problems, of course, is to build more power lines or build them with greater handling capacity. Beginning in 2003, FERC offered incentives for transmission line projects as a shot in the arm to encourage utilities to invest more in the grid. By 2004, utility investment in transmission shot up from $2 billion to $6.5 billion.[30] Specifically, since FERC sets the prices for transmission, FERC offers incentives that guarantee a return on equity. In plain English, transmission utilities get to charge more and these charges are passed on to you.

This doesn't mean they can just string new wires. Rights-of-way must be sited to be big enough to safely transmit high voltage power.

For example, a power line corridor might be the right size to handle towers for 115,000-volt lines (115kV), but be unsuitable for towers holding 230kV or even 345kV lines or higher.

Some of these new rights-of-way pass through national parks, schools, and suburban subdivisions. Many people in various states are fighting these, concerned about potential dangers to the environment, health (through electro-magnetic fields) and property values.

Yet, the bigger threat is that new transmission projects also cost billions of dollars. Consumers ultimately foot the bill through cost-sharing agreements among groups of states. In population-dense areas like the northeast, the cost is spread out around millions of people, appearing as just another fee on monthly usage bills.

But in recent years, the FERC's equity incentive to the transmission industry has gone from a shot in the arm to a heavy dose of sudden-profit steroids. It guarantees them humungous profits for building power lines from generators, a hundred miles away or more.

Case in point: the $2.1 billion, 275 mile-long Potomac-Appalachian Transmission Highline (PATH)[31] which brings a 765kV line across West Virginia into northwestern Maryland. The FERC awarded a return on equity of 14.3 percent, a 100 percent return on construction work-in-progress, and recovery of business startup and administrative costs to AEP and Allegheny Energy.[32] This allows AEP and Allegheny to recoup all their costs, $1.2 billion, by the time PATH is completed in 2014, plus an additional 14.3 percent, totaling about $200 million more.[33]

Another example is the Susquehanna-Roseland transmission line project[34] that stretches from western Pennsylvania into Roseland, New Jersey.

Part of the debate surrounding this project concerns why sufficient additional generation capacity is not being developed in New Jersey. The reason is that the utility building the line will make money for Public Service Enterprise Group (PSEG) while spending millions to upgrade and license its New Jersey nuclear plants.[35]

Rather than building better-planned efficient power generation and modular transmission systems[36], the once moribund transmission industry is shooting FERC's steroid incentives, building its business with bigger, longer projects that earn them billions annually in profits. And their costs will all be added to your bill … again … and again … and again.

Threat #10: Everyone Wants Some

It's hard to imagine life in the 21st century without electricity. In the past 15 years, America's use of electrical power has skyrocketed. We get up in the morning to the frantic beeping of a digital alarm clock. We scrub ourselves clean in our nice hot showers with water from our electric water heaters.

We gulp steaming hot coffee freshly brewed by our digitally-programmed coffee maker as we surf the news sites on the web or listen to the news on our flat-screen TV. We turn on our cell phones and bustle off to work where we sort through megabytes of electronic information, hour after hour.

All the while, generators are spinning, indicator lights are flashing, and high-tension wires are humming as billions of watts of energy flood through the grid to power us through our day at work and at home. Demand for electricity is exploding as the country's population grows. In the past 30 years, urban sprawl has stretched the grid to power condos and convenience stores where cornfields once stood. As people set up their households, they expect to own certain things: a TV, a computer, an alarm clock, a refrigerator, a stove, a water heater, a dishwasher, and air conditioning. And that's just for starters.

Population growth between 2010 and 2020 is projected to be 36 million.[37] That's 36 million more consumers of electricity. These additional 36 million consumers are enough of a strain on the system, but add to that the forecasts of how many people will be moving to the sunbelt – some cities are expected to see an increase of up to 80% in their population[38] – and there will be even more of a strain on the system. That's because in any sunbelt home, the appliance that uses the most electricity is air conditioning. In fact, air conditioning typically eats two-thirds of a home's summer monthly usage.

Do we have enough coal and natural gas to generate electricity … and enough power lines to transmit it … to support 36 million more Americans? ***No.***

Here's why: demand for electricity fluctuates from moment to moment. When demand is highest, usually in the afternoon, many power plants are working at their highest capacity. Sometimes this

Enron and the California Energy Crisis of 2000

In 1996, California deregulated its electricity market. This meant that the once regulated monopoly utilities (Pacific Gas and Electric or PG&E and Southern California Edison) had to abandon their transmission and distribution business and instead concentrate on generating power. Other businesses came to the state and set up shop to handle transmission and distribution.

Hot weather and delays in approving new power plants spiked demand for power. Wholesale prices for electricity rose insanely. Where a megawatt had sold for $45 in 1999, in 2000 it cost $1400. Between April and December of 2000, the wholesale price rose 800%. Deregulation allowed Enron (and other companies) to manipulate the market. Through transmission overbooking and other schemes, Enron (and others) cheated the state of California and its residents out of millions of dollars. Governor Gray Davis declared a state of emergency on January 17, 2001 to deal with the crisis. It would continue until 2003. Ultimately, the state used its power to cap rising electricity prices. Unfortunately, this forced PG&E into bankruptcy and Southern California Edison came close to collapse as well.

As a result, the state suffered many large scale black outs, the governor was ousted from office, and the cost to Californians came to $40 to $45 billion.

peak demand is greater than power plants and transmission lines can handle safely – especially during the summer. This forces ISOs to juggle their resources carefully, often shutting down some areas of the grid altogether. This means extra generators and transmission lines are still needed just to cover present peak demand.

Over the years, utility companies have pulled and stretched the grid like a rubber net to cover the demand of urban sprawl. As a consequence, the grid is even more vulnerable. On average, power plant failures happen twenty percent of the time and can last up to 24 hours. Weather is also causing more and more impact. Brown outs, black outs, and rolling black outs occur more frequently in major cities, are lasting longer, and now cost the nation in lost business more than ever before.

Currently, just enough capacity has been wrung out of the grid to maintain reliability. New transmission lines costing billions of dollars are being planned and constructed. But because their routes challenge state authority and affect

"Over the years, utility companies have pulled and stretched the grid like a rubber net to cover the demand of urban sprawl. As a consequence, the grid is even more vulnerable."

people's homes, these power lines are being fought in the courts.

Preparing for the demand of 36 million more Americans in under 14 years is already straining the entire American energy industry. Utility companies are taking on millions of dollars in debt to prepare for increasing demand and the rising costs of coal and natural gas. International demand, as we've seen, is driving U.S. coal prices higher. The cheap natural gas bubble from too much shale gas drilling will begin dissipating, sending that price higher. In the end, demand will drive up fuel costs, transmission costs, and electricity commodity costs – and those will all be passed onto you.

Did you know ...

February 20, 2015 set a new record for electricity consumption in much of Virginia, as record low temperatures put the grid on the brink of failure. The previous record was a summer day in 2011 when temperatures soared near 100.

(www.fauquiernow.com/)

The Bottom Line

Today, you can plug a lamp or appliance into an outlet in your wall and get electricity on demand. Tomorrow, for any number of reasons, you may not be able to. Will you be ready?

References:

1. http://en.wikipedia.org/wiki/Explosively_pumped_flux_compression_generator
2. http://www.sciencedaily.com/releases/2009/03/090316144521.htm
3. http://lasp.colorado.edu/education/journalists/solar_dynamics_ws/papers/lowres%20Severe%20Space%20Weather%20FINAL.pdf
4. http://homeland.house.gov/Documents/20090722115623-56876.pdf
5. http://www.sciencedaily.com/releases/2010/09/100901073405.htm
6. http://www.sandia.gov/ccss/documents/Cyber_Effects_Analysis_Using_VCSE_09.pdf
7. http://en.wikipedia.org/wiki/Eligible_Receiver_97
8. http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/6805.htm
9. http://online.wsj.com/article/SB123914805204099085.html
10. http://www.reuters.com/article/idUSTRE6AI4HJ20101119
11. http://www.upi.com/Business_News/Security-Industry/2007/06/11/Analysis-Who-cyber-smacked-Estonia/UPI-26831181580439
12. http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf
13. http://www.eia.doe.gov/cneaf/electricity/epm/tableb1.html
14. http://edition.cnn.com/2009/TECH/03/20/smartgrid.vulnerability/
15. http://energyandenvironmentblog.dallasnews.com/archives/2010/03/couple-sues-oncor-over-smart-m.html
16. http://www.keepmecurrent.com/lakes_region_weekly/news/article_2c5601d0-094d-11e0-ab1e-001cc4c002e0.html
17. http://www.indybay.org/newsitems/2010/11/08/18663541.php
18. http://www.forbes.com/2009/10/21/smart-grid-utilities-business-energy-meters.html
19. http://gigaom.com/cleantech/pges-smart-meter-report-a-case-study-of-infrastructure-over-customer/
20. http://www.epa.gov/oust/fedlaws/publ_109-058.pdf
21. http://www.eia.doe.gov/cneaf/electricity/epm/epm_sum.html

22. http://www.eia.doe.gov/cneaf/coal/page/acr/table10.html).
23. http://www.eia.doe.gov/cneaf/coal/page/coalnews/cnmarchive.html
24. http://www.tri-cityherald.com/2010/11/16/1255129/coal-industry-seeks-to-export.html
25. http://www.rigzone.com/news/article.asp?a_id=82017
26. http://www.reuters.com/article/idUSTRE6343RW20100405
27. https://reports.energy.gov/BlackoutFinal-Web.pdf
28. http://www.ee.washington.edu/faculty/radha/dhs_cps.pdf
29. http://congestion09.anl.gov/documents/docs/Congestion_Study_2009.pdf
30. http://fpc.state.gov/documents/organization/122949.pdf
31. http://www.pathtransmission.com
32. http://www.aep.com/environmental/news/?id=1426
33. http://www.aep.com/investors/present/documents/LazardConferenceHandout.pdf
34. http://www.stopthelines.com
35. http://www.foxbusiness.com/markets/2010/11/18/pseg-considering-ma-regulated-segments-drive-growth
36. http://www.pest-03.org/articles/member_application12.htm
37. http://knowledge.wharton.upenn.edu/article.cfm?articleid=1510
38. http://knowledge.wharton.upenn.edu/papers/1319.pdf